Notice of Allowability	Application No.	Applicant(s)	
	10/602,696	AIKAWA ET AL.	
	Examiner	Art Unit	
	Techane J. Gergiso T-G	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☐ This communication is responsive to *11/02/2007*.

2. ☒ The allowed claim(s) is/are *2, 4, 6, 7 and 9*.

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☒ All b) ☐ Some* c) ☐ None of the:
      1. ☒ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

EMMANUEL MOISE
SUPERVISORY PATENT EXAMINER

DETAILED ACTION

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

2. Authorization for this examiner's amendment was given in a telephone interview with applicant's representative Carol Duff on November 16, 2007. The application has been amended as follows:

In claim 6: line 10 and claim 7: line 10, replace "which u" with -- which --.

In claim 2: line 23, claim 6: line 28 and claim 9: line 27 replace "wherein if the command data" with --wherein if command data--.

Reason for allowance

3. After reconsideration of the applicant's remark, filed on November 2, 2007, further search and through examination of the present application, claims 2, 4, 6, 7 and 9 have been found to be in condition for allowance over prior arts of record.

4. The following is an examiner's statement of reasons for allowance:

Claim 2 includes the following features of a smart card which are not taught or further suggested and would not have been obvious over prior arts of record and these features are: An information accumulating unit stores **value data**, **a transfer key** that encrypts the value data, **a transfer key identifier** that verifies whether the transfer key is **newer or older** in accordance with a value of the transfer key identifier, **an update key** that encrypts the transfer key, and **an upper limit of the transfer key identifier** that represents an upper limit of the transfer key identifier that can be stored by the smart card, wherein said arithmetic processing unit **updates the transfer key identifier** and **the transfer key** by performing encryption using the **update key** on the basis of **common-key cryptography**, wherein said arithmetic processing unit **updates the value data** by performing encryption using the **transfer key** on the basis of **the common-key cryptography**.

Claim 4 includes the following features of a smart card which are not taught or further suggested and would not have been obvious over prior arts of record and these features are: An information accumulating unit **stores value data**, **a transfer key** that encrypts the value data, **a transfer key identifier** that verifies whether **the transfer key is newer or older** in accordance with a value of the transfer key identifier, **a first public key certificate** including a **first public key**, which encrypts the transfer key, **a secret key** corresponding to the first public key, and **an upper limit of transfer key identifier** that represents an upper limit of the transfer key identifier which can be stored by the smart card, wherein said arithmetic processing unit **updates the**

transfer key identifier and **the transfer key** by performing encryption using the **first public key certificate and the secret key** on the basis of **public-key cryptography**, wherein said arithmetic processing unit **updates the value data** by performing encryption using the **transfer key** on the basis of **common-key cryptography**.

Claim 6 includes the following features of a smart card which are not taught or further suggested and would not have been obvious over prior arts of record and these features are: An information accumulating unit stores **value data, a transfer key** that encrypts the value data, **a transfer key identifier** that verifies whether **the transfer key is newer or older** in accordance with **a value of the transfer key identifier, an update key** that updates the transfer key, an **update key identifier** that verifies whether **the update key is newer or older** in accordance with a value of **the update key identifier, a first public key certificate** including a **first public key**, which encrypts the transfer key, **a secret key** corresponding to the first public key, and **an upper limit of transfer key identifier** that represents an upper limit of the transfer key identifier which can be stored by the smart card, wherein said arithmetic processing unit **updates the transfer key** by use of the **update key** on the basis of **common-key cryptography**, or **updates the transfer key by** use of **the first public key certificate** and **the secret key** on the basis of **common-key cryptography**, wherein said arithmetic processing **unit updates the value data** by performing encryption using **the transfer key** on the basis of the **common-key cryptography**.

Claim 7 includes the following features of a smart card which are not taught or further suggested and would not have been obvious over prior arts of record and these features are: An information accumulating unit stores **value data**, a **transfer key** that encrypts the value data, **a transfer key identifier** that verifies whether **the transfer key is newer or older** in accordance with a value of the transfer key identifier, **an update key** that updates the transfer key, **an update key identifier** that verifies whether **the update key is newer or older** in accordance with a value of the update key identifier, **a first public key certificate** including a **first public key**, which encrypts the transfer key, **a secret key** corresponding to the first public key, and **an upper limit of transfer key identifier** that represents an upper limit of the transfer key identifier, wherein said arithmetic processing unit **updates the transfer key** by use of the **update key** on the basis of **common-key cryptography**, or **updates the transfer key** by use of **the first public key certificate** and **the secret key** on the basis of **common-key cryptography**, wherein said arithmetic processing unit **updates the value data** by performing encryption using the transfer key on the basis of the **common-key cryptography**.

Claim 9 includes the following features of a smart card which are not taught or further suggested and would not have been obvious over prior arts of record and these features are: An information accumulating unit stores **value data, two or more transfer keys** that encrypts **the value data, a transfer key identifier** that includes **a selection transfer key identifier** that identifies the transfer key currently selected, and that identifies said two or more transfer keys, and an **update key used to update the transfer key**, wherein **if the value of the transfer key identifier**, is **newer than that of said selection transfer key identifier** and , said arithmetic

processing unit **updates said selection transfer key identifier to the transfer key identifier** received by said communication unit by performing encryption using **the update key** on the basis of **common-key cryptography**, wherein said arithmetic processing unit **updates the value data by performing encryption using the transfer key** corresponding to **the update transfer key identifier** on the basis of **common-key cryptography**.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Contact Information

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Techane J. Gergiso whose telephone number is (571) 272-3784 and fax number is (571) 273-3784. The examiner can normally be reached on 9:00am - 6:00pm. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be

obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/T.G/

Art Unit 2137

November 20, 2007

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER